

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/06365

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ G06F15/00 , H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-1999
 Kokai Jitsuyo Shinan Koho 1971-1999 Toroku Jitsuyo Shinan Koho 1994-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, INSPEC, "(proxy+server)*cipher"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP, 8-335207, A (Hitachi, Ltd.), 17 December, 1996 (17.12.96), page 2, left column, lines 2-43 (Family: none)	1, 2, 4, 8-10 3, 6, 7
X	K. Takaragi et al., "Firewall Internet Technology Relating to Firemali (in Japanese)", Tokyo: Shokodo, 10 June, 1998 (10.06.98) p148-152	1, 2, 4, 8-10
Y	JP, 7-212353, A (Nippon Yunishisu K.K.), 11 August, 1995 (11.08.95), page 5, left column, lines 24-45 (Family: none)	3
Y	Naomasa, Minami et al., "Research on the Development of the Platform for Self-decoding type Confidential Information Communication (in Japanese)", Symposium on Cipher and Information Security in 1996, 1996, SCIS96-01C	6, 7
A	JP, 63-220630, A (Matsushita Electric Ind. Co., Ltd.), 13 September, 1988 (13.09.88), page 3; upper right column; lines 4 to 15 (Family: none)	6

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not

considered to be of particular relevance
"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search
09 February, 2000 (09.02.00)Date of mailing of the international search report
29 February, 2000 (29.02.00)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/06365

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>US, 5310999, A (AT&T BELL LAB.), 10 May, 1994 (10.05.94), Full text & EP, 577328, A2 & JP, 6-060237, A & DE, 69321166, E</p>	6

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ G06F15/00, H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996

日本国公開実用新案公報 1971-1999

日本国実用新案登録公報 1996-1999

日本国登録実用新案公報 1994-1999

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

WPI, INSPEC, 「(proxy+server)*cipher」

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P 8-335207, A (株式会社日立製作所), 17. 12 月. 1996 (17. 12. 96), 第2頁左欄第2-43行 (ファミリーなし)	1, 2, 4, 8-10
Y	宝木和夫, 小泉稔, 寺田真敏, 萱島信, 「ファイアウォール インターネット関連技術について」, 東京: 昭晃堂, 10. 6月. 1998 (10. 06. 98) p148-152	3, 6, 7
X	J P 7-212353, A (日本ユニシス株式会社), 11. 8 月. 1995 (11. 08. 95), 第5頁左欄第24-45行 (ファミリーなし)	1, 2, 4, 8-10
Y	南尚鎮, 岡本栄司, 篠田陽一, 満保雅浩. 「自己復号型秘密情報通信のためのプラットフォームの開発研究」 1996年暗号と情報セキュリティシンポジウム, 1996, SCIS96-01C	3
Y		6, 7

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

09. 02. 00

国際調査報告の発送日

29.02.00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

石井 茂和



5M

8837

電話番号 03-3581-1101 内線 6438

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 63-220630, A (松下電器産業株式会社), 13. 9月. 1988 (13. 09. 88), 第3頁, 右上欄, 第4-15 行 (ファミリーなし)	6
A	US, 5310999, A (AT&T BELL LAB.) 1 0. 5月. 1994 (10. 05. 94) 全文&EP, 57732 8, A2&JP, 6-060237, A&DE, 6932116 6, E	6

明 細 書

ネットワーク認証装置および方法

技 術 分 野

本発明は、インターネット等の商用ネットワークにおけるセキュリティ技術に関する。

背 景 技 術

インターネットが商用目的で利用されるようになってくると、ネットワークのセキュリティ技術の早急な確立が必要になってきている。

すなわち、インターネットはTCP/IPによるオープンなプロトコルを用いたデータ通信であり、データ通信の秘密性は本来的に予定されていない。

そのため、公開鍵等の各種の暗号化技術を用いてユーザー端末とサーバとの間のデータセキュリティを確保する技術が多数提案されている。

このような暗号通信では、ユーザー端末から暗号化された特定のデータをサーバに送信し、サーバではこれを復号化して当該ユーザーの正当性を認証するものが一般的であった。

しかし、前記認証サーバそのものはインターネット上でオープンな環境に配置されており、サーバそのものはファイアウォールが確立されていたとしても、そのサーバのアドレスは誰でも知ることができる状態だった。

すなわち、認証サーバは、そのアドレスが公知なことにより、常にハッカーやクラッカーの標的となってしまう可能性を否定できなかった。

さらに、悪意の第三者がこのような暗号化通信を傍受してサーバとの間でデータ通信を再開することにより、いわゆるなりすましが可能となり、クレジットカード等がネットワーク上で不正に使用されてしまう可能性もあった。

本発明は、このような点に鑑みてなされたものであり、認証サーバの存在その

ものの秘密性を高めるとともに、ユーザーが認証のためのデータ入力を行うプログラム自体を使い切り形式にしてユーザー端末に配信することにより、高いネットワークセキュリティを保証するシステムを提供することを技術的課題とする。

発 明 の 開 示

本発明の第1の手段は、データを入力するユーザー端末に対して、当該データを仲介する仲介サーバと、当該データに対して認証を与える認証サーバとからなり、前記ユーザー端末での第1のデータ入力を契機として、暗号化情報を仲介サーバに出力する認証サーバと、前記認証サーバから受信した暗号化情報に基づいて、前記ユーザー端末で入力される第2のデータを暗号化するための暗号化プログラムを生成し、この暗号化プログラムを前記ユーザー端末に配信する仲介サーバとからなるネットワーク認証装置である。

本発明の特徴はこのように「仲介認証システム」を実現した点にある。

すなわち、仲介サーバを経由させることにより、認証サーバの秘匿性を高めることができる。すなわち、認証サーバのアドレスそのものを秘密に保つことができる。

また、認証サーバが有する暗号化情報を仲介サーバに提供し、仲介サーバではこの固有の暗号化情報に基づいて暗号化プログラムを生成し、ユーザー端末から第2のデータが入力されるときに当該暗号化プログラムを通じて暗号化させる。ここで、暗号化プログラムは、J A V Aのアプレットで生成することができる。

なお、ユーザー端末とは、パーソナルコンピュータ等の屋内に設置する形式の端末装置に限らず、携帯電話に接続されて端末機能を有するモバイルコンピュータ、P D A (Personal Data Assistant) 等であってもよい。また、インターネット端末機能を有する携帯電話 (N T T ドコモ株式会社の「iモード端末」等) そのものであってもよい。

本発明の第2の手段は、前記第1の手段において、暗号化情報は暗号化関数とし、前記認証サーバは、暗号化プログラムにより暗号化された第2のデータと、自身が保有する第2のデータを前記暗号化関数で暗号化したものと比較することにより前記ユーザー端末からのセッションの正当性を評価するようにした。

暗号化関数は必ずしも一通りでなくてよく、複数の関数を用意しておくことにより、暗号化による秘匿性がより高められる。

本発明の第３の手段は、前記第１または第２の手段において、暗号化情報は、前記ユーザー端末から仲介サーバへのセッション毎に変化するようにした。

たとえば、認証サーバの機械時計の日時情報をパラメータ（変数）として用いることにより、セッション毎に異なる暗号化情報を生成することができる。これにより、ユーザー端末からのデータを傍受した第三者が不正に仲介サーバにアクセスしても、既に暗号化情報が変化しているために、認証サーバによる正当な認証を受けることができず、秘密が保たれる。

本発明の第４の手段は、前記第１の手段において、前記第１のデータはユーザーＩＤであり、第２のデータはパスワードであることとした。たとえばクレジットカードの獲得ポイント数の確認等において、高い秘匿性が要求されるパスワード情報の転送に本発明を用いることができる。

本発明の第５の手段は、前記第２の手段において、暗号化情報として前記認証サーバのかわりに、前記仲介サーバが有する複数の暗号化関数の中から暗号化関数を特定する暗号化キーにしたものである。

この場合には、認証サーバと仲介サーバとに同一の関数テーブルを有しており、当該暗号化キーによってテーブル中から採用する暗号化関数を特定することができるようになっている。

本発明の第６の手段は、ユーザー端末より受信した第１のデータを仲介サーバにおいて認証サーバに仲介するステップと、前記第１のデータに基づいて暗号化情報を生成し、当該暗号化情報を仲介サーバに送信するステップと、前記第１のデータに対応し認証サーバが保有する第２のデータを読み出してこれを前記暗号化情報で暗号化するステップと、仲介サーバにおいて、前記暗号化情報に基づいて、前記ユーザー端末で入力される第２のデータを暗号化するための暗号化プログラムを生成し、この暗号化プログラムを前記ユーザー端末に配信するステップと、ユーザー端末において、前記暗号化プログラムによって入力された第２のデータを暗号化するステップと、ユーザー端末で暗号化された第２のデータを、前記認証サーバで暗号化された第２のデータと比較するステップとからなるネットワーク認証方法である。

本手段においても、仲介サーバを経由させることにより、認証サーバの秘匿性を高め

ることができる。すなわち、認証サーバのアドレスそのものを秘密に保つことができる。また、認証サーバが有する暗号化情報を仲介サーバに提供し、仲介サーバではこの固有の暗号化情報に基づいて暗号化プログラムを生成し、ユーザー端末から第2のデータが入力されるときに当該暗号化プログラムを通じて暗号化させる。ここで、暗号化プログラムは、J A V Aのアプレットで生成することができる。

本発明の第7の手段は、前記第6の手段において、前記暗号化情報を、前記ユーザー端末から仲介サーバへのセッション毎に変化させるようにした。

たとえば、認証サーバの機械時計の日時情報をパラメータ（変数）として用いることにより、セッション毎に異なる暗号化情報を生成することができる。これにより、ユーザー端末からのデータを傍受した第三者が不正に仲介サーバにアクセスしても、既に暗号化情報が変化しているために、認証サーバによる正当な認証を受けることができず、秘密が保たれる。

本発明の第8の手段は、前記第6の手段で述べたステップからなるプログラムを記憶した記憶媒体である。

ここで、記憶媒体とは、光学的、磁氣的、光磁氣的な記録手段を備えたあらゆる媒体を含み、光ディスク、光磁気ディスク、磁気テープ、またはこれらを収容したカートリッジ、カセット、カード等を含む。

本発明の第9の手段は、認証サーバはユーザー端末での処理要求の入力を契機にこの処理要求に対する固有情報を発生させ、これを受け取った仲介サーバは、前記固有情報に基づいて生成した入力インターフェースを前記ユーザー端末に提供するものである。

処理要求とは、たとえばインターネットブラウザ等に表示されるボタンをユーザーがマウスで指示することにより送信される行為を意味する。認証サーバで発生させる固有情報とは、たとえば当該処理要求に対応する受付番号や暗号化方法等を意味する。

本発明の第10の手段は、前記第9の手段において、前記入力インターフェースとしてユーザー端末上で機能する実行プログラムを用意し、この実行プログラ

ムでは2以上のユーザー情報の入力を受け付けてこれらを暗号化して前記仲介サーバに送信するようにしたものである。

実行プログラムとは、たとえばJ A V A アプレットであり、ユーザー情報とはこのアプレット上で入力されるカード番号や暗証番号を意味する。これらのユーザー情報は、当該アプレット上で暗号化されて仲介サーバを経て認証サーバに送られる。

図面の簡単な説明

図1は、本発明の実施形態におけるシステム構成を示す概略図

図2は、受付データベースの内容を示す説明図

図3は、オーソリデータベースの内容を示す説明図

図4は、実施形態の受付処理における仲介サーバと認証サーバの機能ブロック図

図5は、実施形態の認証処理における仲介サーバと認証サーバの機能ブロック図

図6は、実施形態において、ユーザー端末に提供されるHTMLファイルと暗号化アプレットの生成手順を示すブロック図

図7は、実施形態において、ユーザー端末に提供されるHTMLファイルのソースコードを示す説明図

図8は、実施形態の仲介サーバでの暗号化アプレットの生成方法の変形例を示すブロック図

図9は、実施形態の暗号化テーブルを示す説明図(1)

図10は、実施形態の暗号化テーブルを示す説明図(2)

図11は、実施形態の暗号化テーブルを示す説明図(3)

図12は、実施形態のアプレットのテンプレートを示す説明図

図13は、実施形態においてユーザー端末と仲介サーバと認証サーバとの間のデータのやりとりを示すシーケンス図

図14は、実施形態のユーザー端末の表示画面(1)

図15は、実施形態のユーザー端末の表示画面(2)

図16は、実施形態のユーザー端末の表示画面(3)

図 17 は、実施形態のユーザー端末の表示画面（4）

図 18 は、実施形態の変形例におけるユーザー端末と仲介サーバと認証サーバとの間のデータのやりとりを示すシーケンス図（1）

図 19 は、実施形態の変形例におけるユーザー端末と仲介サーバと認証サーバとの間のデータのやりとりを示すシーケンス図（2）

発明を実施するための最良の形態

以下本発明を図面に基づいて説明する。

図 1 は、本実施形態のシステム構成を示す概略図である。

本実施形態は、ユーザー端末 1 がインターネット 2 を介して仲介サーバ 3 に接続されており、この仲介サーバ 3 はファイアウォールサーバ 4 を介して LAN または WAN によって認証サーバ 5 と接続されている。

このユーザー端末 1 は、パーソナルコンピュータ等の屋内に設置する形式の端末装置に限らず、携帯電話に接続されて端末機能を有するモバイルコンピュータ、PDA（Personal Data Assistant）等であってもよい。また、インターネット端末機能を有する携帯電話（NTTドコモ株式会社の「iモード端末」等）そのものも用いることができる。

認証サーバ 5 は、受付データベース 6 とオーソリデータベース 7 とを有しており、各データベースのファイル構成は図 2 および図 3 に示す通りとなっている。すなわち、受付データベース 6 には、認証サーバ 5 で付与される受付番号と、ユーザー端末 1 で入力されたカード番号と、暗号化アルゴリズムを特定するための暗号化キー（後で詳述する）が登録されている。また、オーソリデータベース 7 には、認証のためにあらかじめ登録されているカード番号と、同じくあらかじめ登録されているパスワードとが登録されている。

なお、認証サーバ 5 には、前記受付データベース 6 とオーソリデータベース 7 以外にも、ユーザー情報データベース 26 および認証結果データベース 27（ともに図 5 参照）を有しているが、図 1 では図示を省略している。

前記図 1 に示したシステムは、たとえば、ユーザーが、ユーザー端末 1 よりクレジットカードの番号およびパスワードを入力することにより、当該クレジット

カートに累積されたポイント（得点）を参照するために用いられる。ユーザー端末1から入力されるクレジットカード番号やパスワードは、通信路上で高いセキュリティが必要であり、またこれを認証するための認証サーバ5も受付データベース6やオーソリデータベース7のセキュリティを維持する必要がある。

本実施形態では、これらの点について、ユーザー端末1から入力されるクレジットカード番号やパスワードを一時的な使い切りプログラム、たとえば使い捨てのJ A V Aアプレットを用いて通信路上のデータ傍受を防止するとともに、仲介サーバ3を設けてユーザー端末1は直接的にはこの仲介サーバ3と通信することにより、認証サーバ5そのもののアドレスやシステム構成を秘密化している。

次に、図4を用いてユーザー端末1と仲介サーバ3と認証サーバ5のそれぞれの機能について説明する。

図4は、ユーザー端末1が仲介サーバ3のサーバプログラム12にアクセスして（図14参照）、カード番号入力画面（図15参照）を選び、カード番号を仲介サーバ3に送信し、図16に示した暗証番号入力画面がユーザー端末1に表示されるまでのユーザー端末1と仲介サーバ3と認証サーバ5との各機能分担を示したブロック図である。

まず、ユーザーは、ユーザー端末1よりインターネット2にダイヤルアップIP等の方法でアクセスし、ユーザー端末1内のブラウザ11（WWW閲覧プログラム）を起動する。そして、URL（Uniform Resource Locator）として仲介サーバ3のサーバプログラム12のアドレスを指定することによって、図14に示す画面が表示される。

そして、ユーザーが図14に示した画面上でポイント照会をマウス等の入力補助装置を用いて指定することによって、当該「ポイント照会」に設定されたリンク情報にしたがって、図15に示すカード番号入力画面が表示される。

ここで、ユーザーが自身のカード番号（たとえば「1234」）を入力すると、この入力されたカード番号（ID）が仲介サーバ3に送信される（図4のステップ(1)：以下、本実施態様におけるカッコ付き数字は、図4の丸付き数字に対応する）。

仲介サーバ3のサーバプログラム12が前記カードIDを受け取ると、受付サーバブレット13（使い切りのサーバ側プログラム）を起動して（ステップ(2)）、

カードIDを受付サーバ13を介してキューイング14の状態にする（ステップ(3)，(4)）。

認証サーバ5は、キューフェッチ機能15により仲介サーバ3からのキューを定期的にチェックしており（ステップ(5)）、前記キュー14を確認するとこれを取り込む（ステップ(6)）。

そして、認証サーバ5は、オーソリ・ユーザー・エージェント・プログラム（以下、「オーソリUA」という）16を起動するとともに、このオーソリUA16に対してカードIDを送信する（ステップ(7)，(8)）。このオーソリUA16は一時的なエージェント・プログラムであり、ユーザー端末1よりなんらかの理由で通信が切断された場合には、一定時間経過後に認証サーバ5上から削除される。

オーソリUA16は、さらに、認証サーバ5の暗号化関数管理部17より暗号化キーと暗号化関数を読み出して（ステップ(9)）、受付番号を生成し、受付情報を受付データベース6に格納する（ステップ(10)）。なお、暗号化キーとは、暗号化するための鍵情報を意味し、複数の暗号化関数の中からアクセス毎に択一的に採用されたものを用いる。

このような暗号化キーを用意しておく理由は以下の通りである。

すなわち、カードIDは一定であるため、同一のカードIDで複数回のアクセスがあることが考えられる。そのため、カードIDに対してアクセス毎に異なる暗号化キーを実現できる複数の暗号化関数を用意しておくことにより、不正アクセスを防止できる。

なお、暗号化キーと暗号化関数については、図9，10および11を用いて後述する。また、受付番号は、シーケンシャルな番号であり、毎日午前零時にリセットされる。すなわち、その日の3番目のアクセスには「0003」が付与される。

オーソリUA16は、前記のように受付順に付与される受付番号を生成し（ステップ(10)）、前記カードIDと暗号化キーとともに受付データベース6に格納する（図2参照）。

次に、オーソリUA16は、仲介サーバ3に対して仲介ユーザー・エージェント（以下、「仲介UA」という）20の起動を指示する（ステップ(11)，(12)）。

仲介サーバ3内で仲介U A 2 0が起動されると、前記認証サーバ5のオーソリU A 1 6から受付番号、カードID、暗号化関数からなる受付情報を送信する（ステップ(13)）。

この受付情報を受け取った仲介U A 2 0は、前述の受付サブレット1 3に対して受付番号と暗号化関数を送信する（ステップ(14)）。

受付サブレット1 3は、これに基づいて、受付番号と暗号化関数を埋め込んだ暗号化アプレット2 1を生成する（ステップ(15)）。この暗号化アプレット2 1はサーバプログラムを通じてユーザー端末1のブラウザ1 1に送信される（ステップ(16), (17)）。

この暗号化アプレット2 1とは、いわゆるJ A V Aアプレットであり、インターフェースとしてのH T M L (Hyper Text Mark-up Language)ファイルとともにユーザー端末1のブラウザ1 1に送信される。このときのブラウザ1 1の画面を示したものが図1 6である。これを表示するためのH T M Lファイルは、図7に示すようにテキストの記述で構成されている。この記述中、APPLET CODEとして指定されているOTP19980812114910.classが暗号化アプレット2 1のファイル名となっている。この暗号化アプレット2 1は、いわゆるワン・タイム・プログラムであり、当該カードIDの認証のためのセッションのみに用いられる一時的なプログラムである。暗号化アプレット2 1は、前述のように、認証サーバ5で付与された受付番号と、暗号化関数によって生成されているため、同一の暗号化アプレット2 1が生成される可能性は天文学数値的に低くなっている。

次に、図5を用いて、ユーザー端末1のブラウザ1 1上で、図1 6に示したアプレット画面で入力されたパスワードが、仲介サーバ3を経由して認証サーバ5で認証されて図1 7に示すような認証画面が表示されるまでの仲介サーバ3と認証サーバ5との機能を説明する。

まず、ユーザー端末1上のブラウザ1 1より入力されたパスワードは、前述のように1回のセッションだけのために生成された前記暗号化アプレット2 1によって暗号化されて仲介サーバ3に送信される（ステップ(2)）。このように仲介サーバ3から提供された1回限りの暗号化アプレット2 1を用いて入力されたパスワードを暗号化することによって、ユーザー端末1と仲介サーバ3との回線をトレースして当該通信を傍受したとしても、同一のカードIDによる次のセッショ

ンには利用することができない。

前記暗号化パスワードを受信した仲介サーバ3では、サーバプログラム12によって認証サブレット25が起動され、ここに前記暗号化パスワードが引き渡される(ステップ(3)、(4))。

ここで、認証サブレット25は、図4で説明した受付サブレット13が保有していた受付番号を引き継ぎ、暗号化パスワードとともにこの受付番号を仲介UA20に送信する(ステップ(5))。

認証サーバ5のオーソリUA16からは一定間隔で仲介サーバ3に対して認証要求がなされており(ステップ(1))、仲介サーバ3の仲介UA20が前述の受付番号と暗号化パスワードを受け取った状態になっていると、この認証要求をトリガとしてこれらの情報をオーソリUA16に送信する(ステップ(6))。

オーソリUA16は、前記受付番号をキーにして受付データベース6にアクセスし、この受付番号に対応するカードIDと暗号化キーを読み出す(ステップ(7))。そして、得られたカードIDと暗号化キーと前記の暗号化パスワードを組にして認証部28に対して認証要求を行う(ステップ(8))。

前記認証要求を受け付けた認証部28は、暗号化関数管理部17より暗号化関数を読み出すとともに(ステップ(9))、オーソリデータベース7よりカードIDをキーにしてパスワードを読み出す(ステップ(10))。そして、認証部28は、オーソリデータベース7から読み出したパスワードを暗号化関数によって暗号化し(ステップ(11))、これをオーソリUA16が受信した暗号化パスワードと比較する(ステップ(12))。

認証部28は、前記両暗号化パスワードが一致した場合には、認証OKとして、ユーザー情報データベース26よりユーザー情報を読み出す(ステップ(13))。このユーザー情報とは、たとえば当該ユーザーのクレジットカードに対する獲得ポイント数などである。そして、認証部28は、認証結果データベース27にこの認証結果として、受付番号、暗号化パスワードおよびユーザー情報を登録する(ステップ(14))。これとともに、オーソリUA16に対して認証結果、すなわち認証OKの結果フラグと獲得ポイント数等のユーザー情報を送信する(ステップ(15))。

オーソリUA16は、認証結果がOKだった場合には、受付データベース6に

暗号化パスワードを書き込むとともに（ステップ(16)）、仲介サーバ3の仲介U A 2 0に対して認証結果をユーザー情報とともに送信する（ステップ(17)）。

前記認証結果は、仲介サーバ3の仲介U A 2 0→認証サーバレット2 5およびサーバプログラム1 2を経由してユーザー端末1に送信され、当該ユーザー端末1上のブラウザ画面に表示される（ステップ(18)～(20)）。

このときのユーザー端末1上の表示画面を示したものが図1 7である。

次に、図4で説明したブラウザ1 1に提供されるHTMLファイルと暗号化アプレット2 1の生成手順について図6を用いて説明する。

まず、前述のように、ブラウザ1 1上よりカードIDが入力されると（ステップ(1)）、サーバプログラム1 2が起動し、受付サーバレット1 3の起動が促される（ステップ(2)）。

受付サーバレット1 3は、まず、図1 2に示すようなアプレットのテンプレート6 1を選択的に読み出して（ステップ(3)）、種プログラム(Seed)の書き換えと実行ファイル(class)の出力を行い（ステップ(4)）、暗号化アプレット2 1を生成する。そして、この暗号化アプレット2 1は、受付サーバレット1 3によって生成されたHTMLデータ6 2とともに、サーバプログラム1 2を通じてユーザー端末1のブラウザ1 1に提供される（ステップ(5)～(6)）。

このHTMLデータ6 2の具体的なソースコードを示したものが図7である。

次に、本実施形態における暗号化について説明する。

まず、前記暗号化アプレット2 1を当該セッション限りの使い切りとするため、暗号化キーを設定する。すなわち、暗号化キーの操作によってセッション毎に異なる暗号化式を生成させることになる。そのため、暗号化関数管理部1 7には、図9および図1 0に示す暗号化関数を登録した暗号化テーブルAおよびBが設けられている。

すなわち、本実施形態では、暗号化キーによって採用される暗号化関数が特定されるようになっており、この暗号化キーは後の認証のために認証サーバ5の受付データベース6内に保持される（図5参照）。

図9および図1 0において、変数aは日付であり、各サーバが有している時計機能から得る。当該テーブル構成において、暗号化キーとして「A 3」が指定されたときには、図9に示すテーブルAの3番目の式、すなわち、「 $Y = aX + 3$ 」

が採用される。この式を用いた場合、たとえば当該日が10日であるとする
($a = 10$)、入力された数値 X を10倍して3を加えた数値 Y が暗号化値となる。

なお、暗号化キーは、セッション毎に異なる数値が生成されるように、変数としてサーバの機械時計の値を用いてもよい。たとえば、暗号化テーブルに図11に示すような関数が登録されている場合、 A はサーバの機械時計の秒(4桁)、 B はサーバの機械時計の年月日(6桁)、 C はサーバの機械時計の時分(4桁)としてもよい。

次に、図13を参照しながら、本実施形態における暗号化と認証の理解を容易にするために、以下の具体的な数値を用いてユーザー端末1と、仲介サーバ3と、認証サーバ5とのやりとりを時系列的に説明する。

カード番号(ID) : 1234

受付番号 : 4912

パスワード : 9104

暗号化関数 : $Y = 3X - 99$

まず、ユーザー端末1よりカード番号(ID)として「1234」が入力されると(ステップ1301)、仲介サーバ3はこれを仲介して(1302)、認証サーバ5に通知する。

認証サーバ5では、このカード番号(ID)「1234」を取得し、これに受付番号「4912」を付与する。そして、暗号化方法を設定する(1303)。具体的には暗号化関数「 $Y = 3X - 99$ 」とこの関数を特定する暗号化キーが暗号化関数管理部17から読み出される(図4参照)。

仲介サーバ3は認証サーバ5より前記受付番号「4912」と暗号化関数「 $Y = 3X - 99$ 」を取得し(1304)、これらを埋め込んだ暗号化アプレット21を生成する(1305)。

次に、ユーザー端末1上でパスワード「9104」が入力されると(1306)、これが暗号化関数「 $Y = 3X - 99$ 」によって計算され、計算結果が暗号化暗証番号「27213」として仲介サーバ3を通じて認証サーバ5に通知される(1

307, 1308)。

一方、認証サーバ5では、前記と並行して、前記暗号化関数「 $Y = 3X - 99$ 」を暗号化関数管理部17から読み出すとともに(1309)、ステップ1303で取得したカード番号(ID)をキーにしてオーソリデータベース7よりパスワード「9104」を読み出す(1310)。そして、読み出されたパスワードを、前記暗号化関数「 $Y = 3X - 99$ 」によって暗号化する(1311)。そしてここで暗号化された数値と前述のユーザー端末1から通知された暗号化暗証番号「27213」と比較する(1312)。

この結果、オーソリデータベース7に格納されていたパスワードを暗号化したものと、ユーザー端末1からの暗号化暗証番号とが一致した場合には認証が成立して認証サーバ5内で保持されていたユーザー情報が仲介サーバ3を介して(1313)、ユーザー端末1に提供される(1314)。

なお、以上の説明は認証サーバ5から暗号化関数を仲介サーバ3に通知して暗号化アプレット21を生成する場合であったが、図8に示すように、仲介サーバ3が認証サーバ5から暗号化キー801のみを受け取り、仲介サーバ3自身が有する関数テーブル802との組み合わせで暗号化アプレット21を生成してもよい。

この場合、仲介サーバ3が保持する関数テーブル802は、認証サーバ5が有する暗号化関数管理部17の関数テーブルと同一のものでなければならない。

図18は、本発明の実施形態の変形例におけるユーザー端末と仲介サーバと認証サーバとの間のデータのやりとりを示すシーケンス図である。

前述の図13のシーケンス図では、ユーザー端末1よりカード番号を入力した後に認証サーバで受付番号が発行され、これに基づいて仲介サーバ3でアプレットが生成・配信され、ユーザー端末1上ではこのアプレット上で暗証番号を入力するようになっていた。

これに対して、図18のシーケンスでは、ユーザー端末1で処理要求がなされると、認証サーバ5からの受付番号・暗号化方法に基づいて仲介サーバ3でアプレットが生成・配信され、ユーザー端末1上ではこのアプレット上でカード番号と暗証番号を入力するようになっている。

これを具体的に説明する。

ま 9、ユーザー端末 1 にてユーザーがインターネットノフワサ等を通じて表示された処理要求のボタンをマウスでクリックすると（ステップ 1801）、仲介サーバ 3 は、この処理要求があったことを認証サーバ 5 に通知する（1802）。認証サーバ 5 では、これに基づいて受付番号と暗号化方法（たとえば、暗号化関数「 $Y = 3X - 99$ 」）を設定する（1803）。このステップ 1803 の処理は前述の図 13 のステップ 1303 と同様である。ここで、たとえば受付番号として 4912 が認証サーバ 5 に付与されたとすると、この受付番号と暗号化方法とが仲介サーバ 3 に通知される（1804）。

仲介サーバ 3 ではこれに基づいて、アプレットを生成しユーザー端末 1 に配信する（1805）。

ユーザー端末 1 上では、仲介サーバ 3 から配信されたアプレットが実行され、ユーザーからカード番号と暗証番号の入力を受け付ける（1806）。ここで、入力された暗証番号は、前述の暗号化方法に基づいてアプレット上で暗号化暗証番号（ここでは、 $Y = 3X - 99 = 3 \times 9104 - 99 = 27213$ ）に変換されて仲介サーバ 3 に送られる（1807）。

一方、認証サーバ 5 では、前記と並行して、前記暗号化関数「 $Y = 3X - 99$ 」を暗号化関数管理部 17 から読み出すとともに（1809）、対象となるデータをオーソリデータベース 7 より読み出す（1810）。これには、カード番号とパスワード「9104」が含まれる。そして、読み出されたパスワードを、前記暗号化関数「 $Y = 3X - 99$ 」によって暗号化する（1811）。そしてここで暗号化された数値と前述のユーザー端末 1 から通知された暗号化暗証番号「27213」と比較する（1812）。

この結果、オーソリデータベース 7 に格納されていたパスワードを暗号化したものと、ユーザー端末 1 からの暗号化暗証番号とが一致した場合には認証が成立して認証サーバ 5 内で保持されていたユーザー情報が仲介サーバ 3 を介して（1813）、ユーザー端末 1 に提供される（1814）。

このように図 18 に示した変形例では、ユーザーに対してカード番号と暗証番号を同じアプレット上で入力させるため、カード番号を入力してから暗証番号の入力画面を待つというようなユーザーにストレスを感じさせることがない。

また、図 18 ではステップ 1806 のアプレット上でカード番号と暗証番号の

2つのユーザー情報を入力する例を示したが、ユーザー情報はこれらの2つに限られず、複数の項目を入力させるようにしてもよい。この例をシーケンス図で示したものが図19である。同図に示すように、オーソリデータベース7には複数の項目のデータが登録されており、これらと入力されたユーザー情報が照合されることになる。

なお、詳細は図13および図18で説明したものと同様であるので説明は省略する。

以上説明したように、本発明によれば、ユーザー端末からの認証業務に対して、仲介サーバを経由することにより認証サーバの存在そのものを秘密化できる。

また、仲介サーバによって当該セッション限りの使い切りの暗号化プログラムを提供し、この暗号化プログラムによってユーザー端末上で入力データを暗号化できるため、通信路上での漏洩に対してもセキュリティの高いデータ通信が可能となる。

さらに、前記暗号化プログラムは当該セッション限りの使い切りの暗号化プログラムであるため、漏洩したデータに基づいて第三者がセッションを開始しても暗号化プログラムが一致することはなく、不正アクセスを防止できる。

産業上の利用可能性

本発明は、ユーザーが端末コンピュータや携帯端末からインターネットを経由した商品購入等の場合の認証システムに利用できる。

請 求 の 範 囲

1. データを入力するユーザー端末に対して、当該データを仲介する仲介サーバと、当該データに対して認証を与える認証サーバとからなり、

前記ユーザー端末での第1のデータの入力を契機に、暗号化情報を仲介サーバに出力する認証サーバと、

前記認証サーバから受信した暗号化情報に基づいて、前記ユーザー端末で入力される第2のデータを暗号化するための暗号化プログラムを生成し、この暗号化プログラムを前記ユーザー端末に配信する仲介サーバとからなるネットワーク認証装置。

2. 前記暗号化情報は暗号化関数であり、前記認証サーバは、暗号化プログラムにより暗号化された第2のデータと、自身が保有する第2のデータを前記暗号化関数で暗号化したものと比較することにより前記ユーザー端末からのセッションの正当性を評価することを特徴とする請求項1記載のネットワーク認証装置。
3. 前記暗号化情報は、前記ユーザー端末から仲介サーバへのセッション毎に変化することを特徴とする請求項1または2記載のネットワーク認証装置。
4. 前記第1のデータはユーザーIDであり、第2のデータはパスワードであることを特徴とする請求項1記載のネットワーク認証装置。
5. 前記暗号化情報は、前記認証サーバのかわりに前記仲介サーバが有する複数の暗号化関数の中から暗号化関数を特定する暗号化キーであることを特徴とする請求項2記載のネットワーク認証装置。
6. ユーザー端末より受信した第1のデータを仲介サーバにおいて認証サーバに仲介するステップと、

前記第1のデータに基づいて暗号化情報を生成し、当該暗号化情報を仲介サーバに送信するステップと、

前記第1のデータに対応し認証サーバが保有する第2のデータを読み出してこれを前記暗号化情報で暗号化するステップと、

仲介サーバにおいて、前記暗号化情報に基づいて、前記ユーザー端末で

入力される第2のデータを暗号化するための暗号化プログラムを生成し、この暗号化プログラムを前記ユーザー端末に配信するステップと、

ユーザー端末において、前記暗号化プログラムによって入力された第2のデータを暗号化するステップと、

ユーザー端末で暗号化された第2のデータを、前記認証サーバで暗号化された第2のデータと比較するステップとからなるネットワーク認証方法。

7. 前記暗号化情報は、前記ユーザー端末から仲介サーバへのセッション毎に変化することを特徴とする請求項6記載のネットワーク認証方法。

8. ユーザー端末より受信した第1のデータを仲介サーバにおいて認証サーバに仲介するステップと、

前記第1のデータに基づいて暗号化情報を生成し、当該暗号化情報を仲介サーバに送信するステップと、

前記第1のデータに対応し認証サーバが保有する第2のデータを読み出してこれを前記暗号化情報で暗号化するステップと、

仲介サーバにおいて、前記暗号化情報に基づいて、前記ユーザー端末で入力される第2のデータを暗号化するための暗号化プログラムを生成し、この暗号化プログラムを前記ユーザー端末に配信するステップと、

ユーザー端末において、前記暗号化プログラムによって入力された第2のデータを暗号化するステップと、

ユーザー端末で暗号化された第2のデータを、前記認証サーバで暗号化された第2のデータと比較するステップとからなるプログラムを記憶した記憶媒体。

9. データを入力するユーザー端末に対して、当該データを仲介する仲介サーバと、当該データに対して認証を与える認証サーバとからなり、

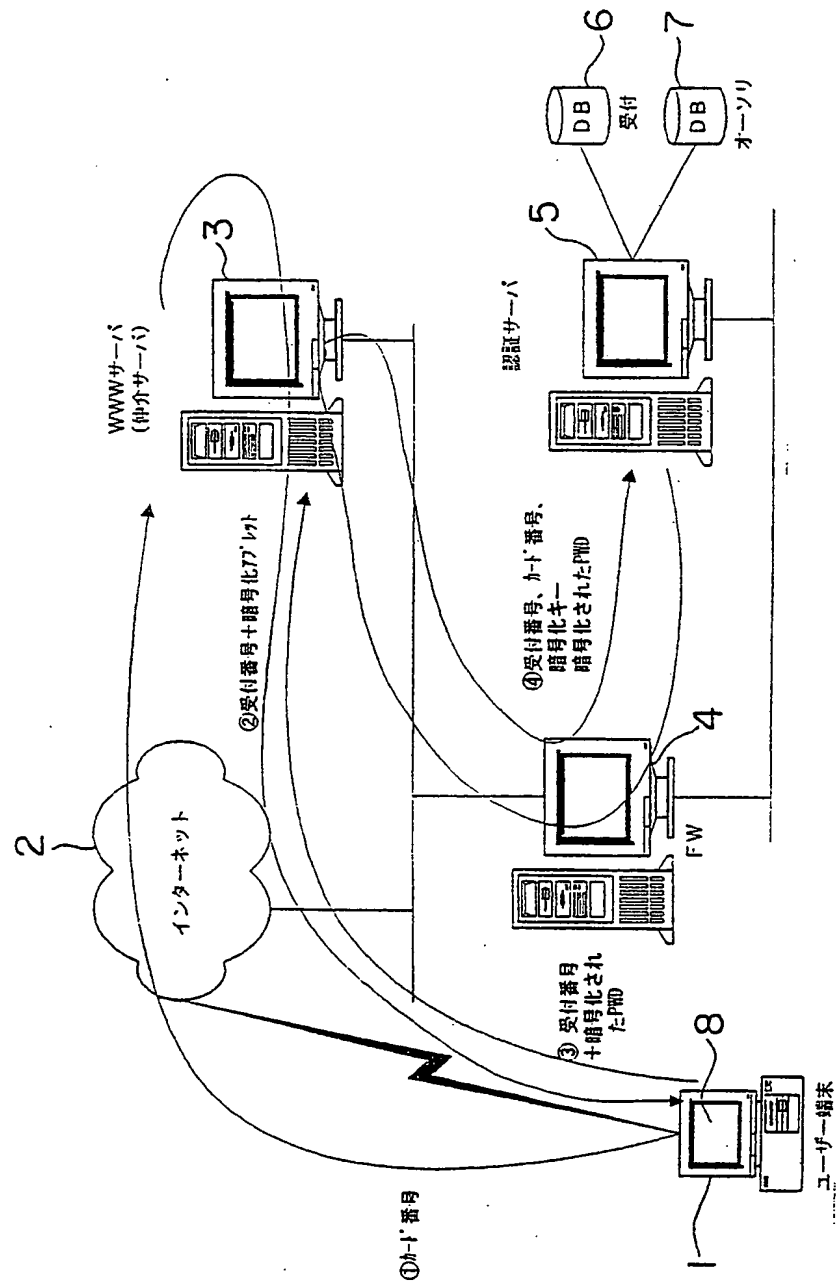
前記ユーザー端末での処理要求の入力を契機に、前記処理要求に対する固有情報を発生させる認証サーバと、

前記固有情報に基づいて生成した入力インターフェースを前記ユーザー端末に提供する仲介サーバとからなるネットワーク認証装置。

10. 前記入力インターフェースは、ユーザー端末上で機能する実行プログラムであり、

当該実行プログラムは２以上のユーザー情報の入力を受け付けるとともに、

前記で入力された２以上のユーザー情報を暗号化して前記仲介サーバに送信する請求項９記載のネットワーク認証装置。



This Page Blank (uspto)

図 2

<受付DB>

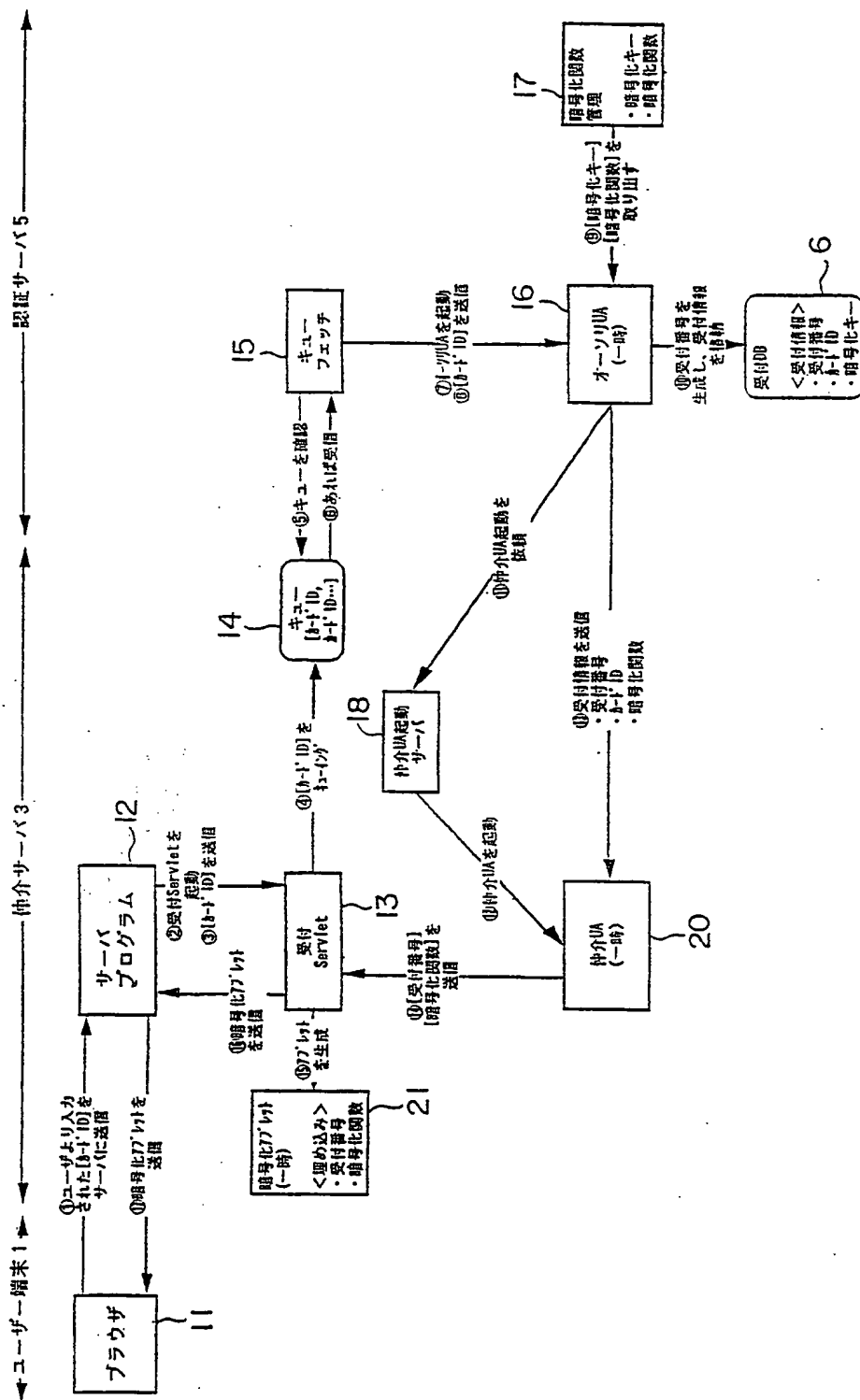
受付番号	認証サーバで打番された受付のための番号
カードID	ユーザによって入力されたカード番号
暗号化キー	暗号化アルゴリズムを特定するためのキー

【図 3】

<オーソリDB>

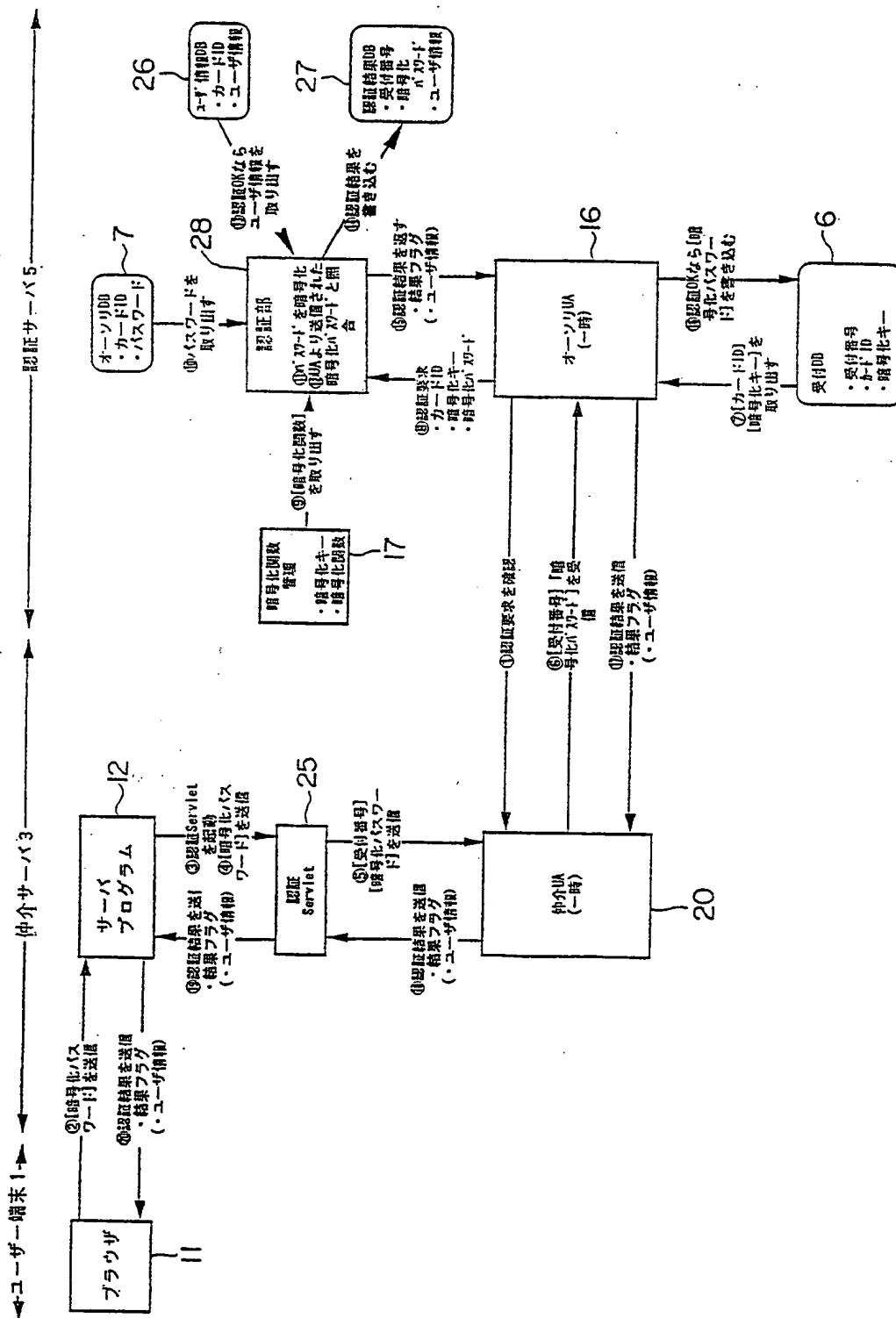
カードID	あらかじめ登録されているカード番号
パスワード	あらかじめ登録されているパスワード

This page Blank (uspto)



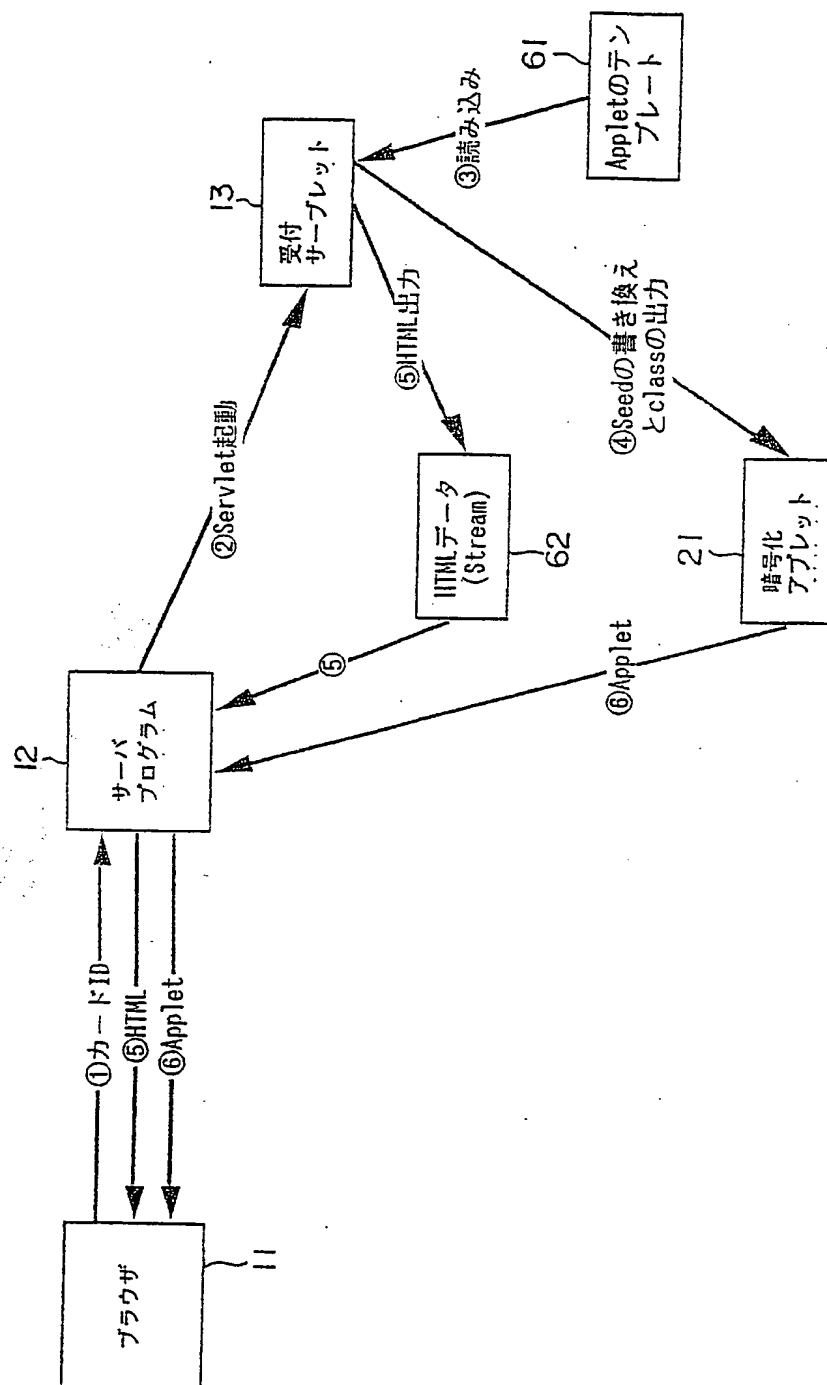
This page Blank (uspto)

図 5



This page Blank (uspto)

図 6



This page Blank (uspto)


```
<HTML>
<HEAD>
<TITLE>パスワード入力画面</TITLE>
</HEAD>
<BODY>
```

.....

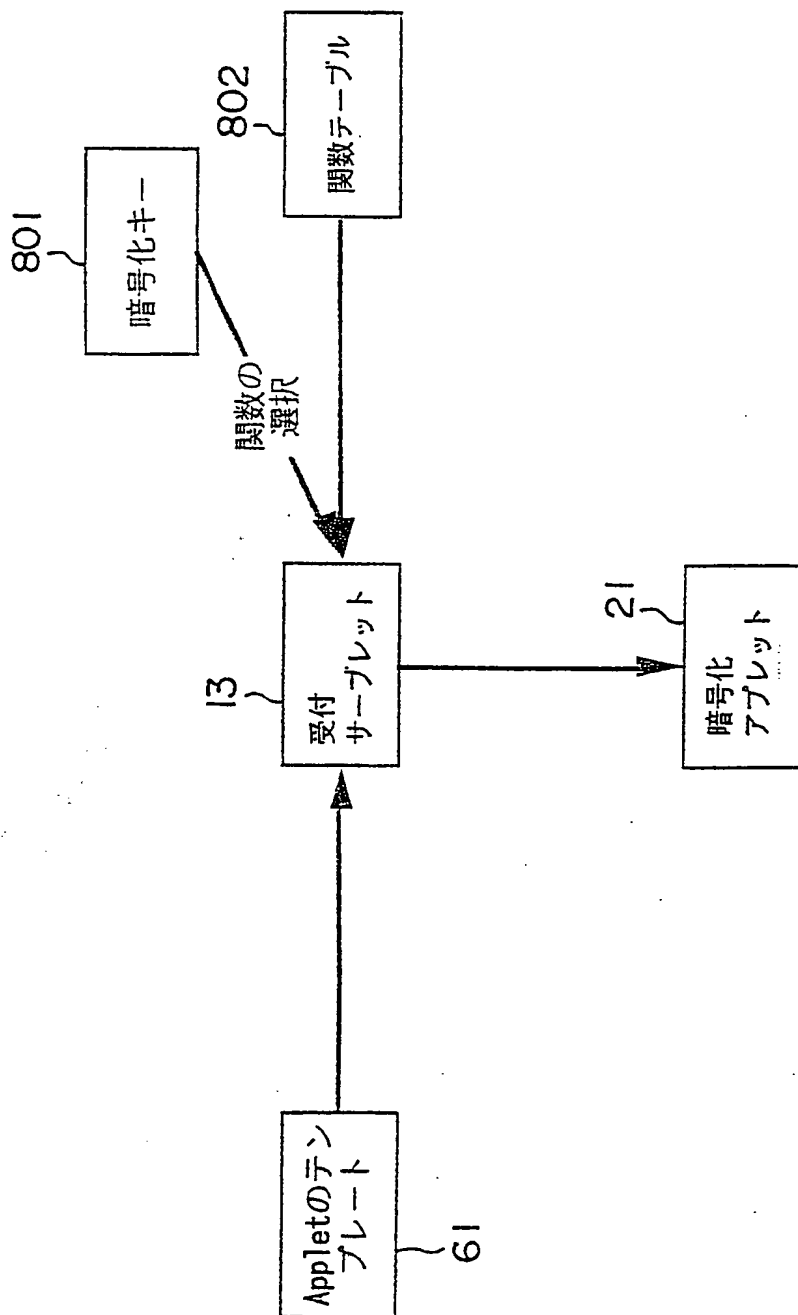
```
<APPLET CODE="OTP19980812114910.class" WIDTH=400 HEIGHT=300>
</APPLET>
```

.....

```
</BODY>
</HTML>
```

62

This page Blank (uspto)



This page Blank (uspto)

図 9

table A

1	$Y = aX + 2$
2	$Y = aX + 9$
3	$Y = aX + 3$

a : マシン日付の日を使用する

図 10

table B

4	$Y = bX + 5$
5	$Y = bX + 7$
6	$Y = bX + 6$

b : マシン日付の月を使用する

This page Blank (uspto)

図 1 1

日付の下1桁が1, 4, 7	$Y = AX + B + C$
日付の下1桁が2, 5, 8	$Y = (A+B)X + C$
日付の下1桁が3, 6, 9	$Y = (A+C)X + B$
日付の下1桁が0	$Y = (A+B+C)X + A$

図 1 2

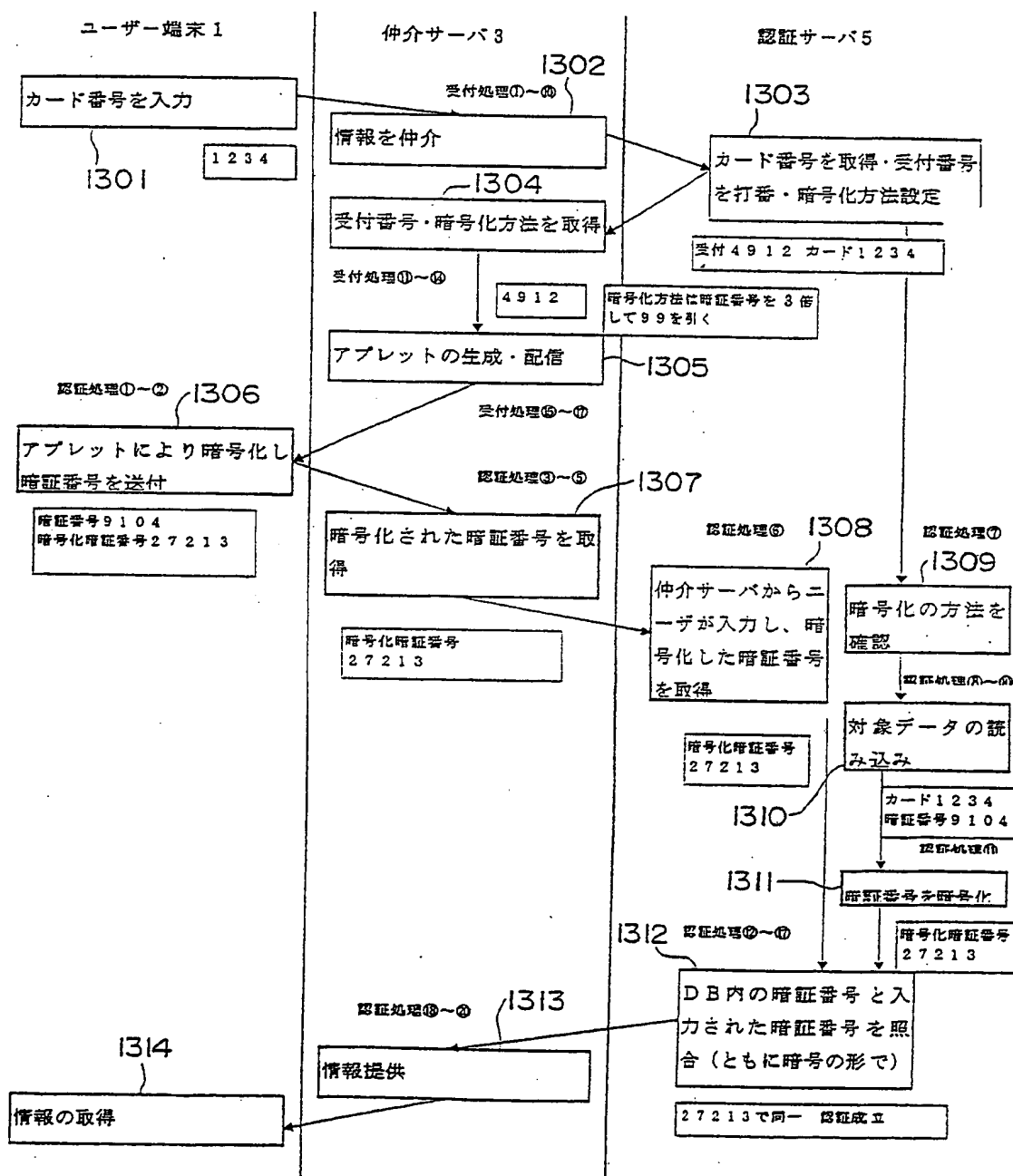
ユーザIDを入力してください

Submit Reset

61

This Page Blank (uspto)

図 13



Page Blank (uspia)

図 1 4

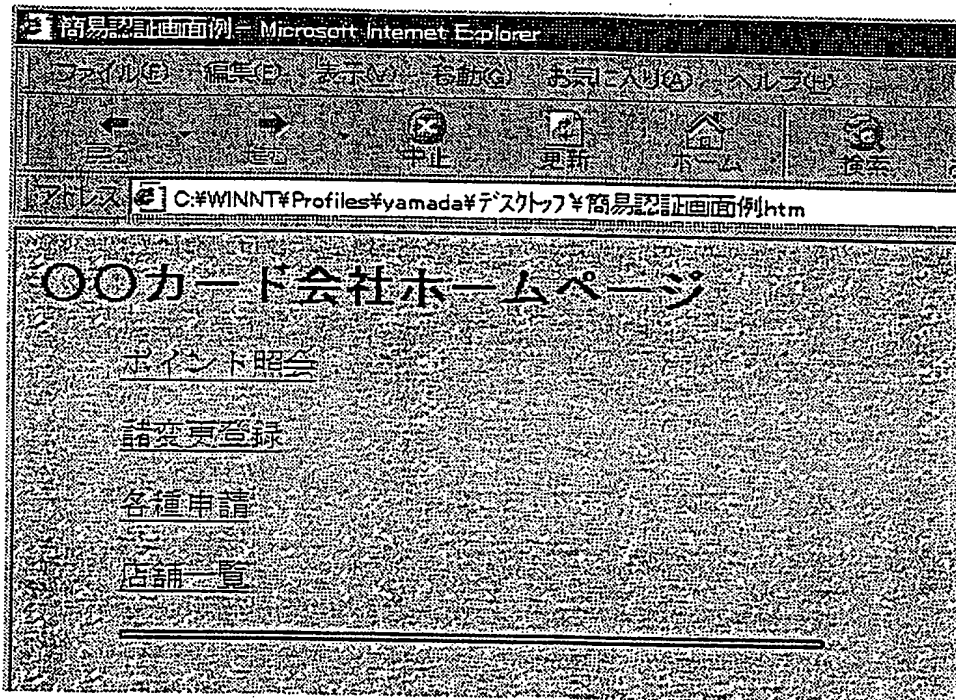
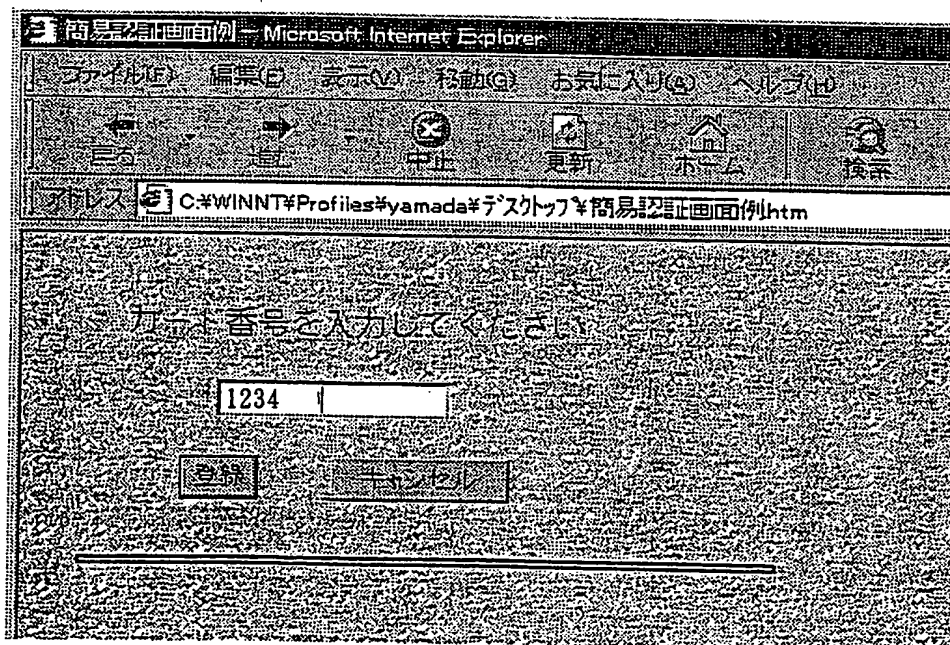


図 1 5



This Page Blank (uspto)

図 16

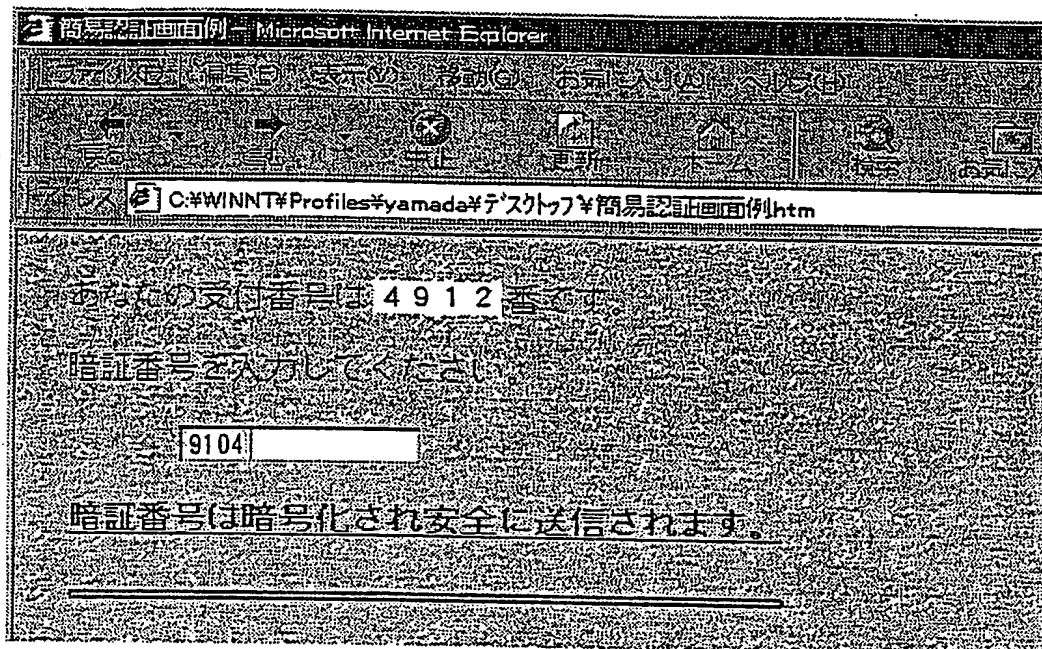
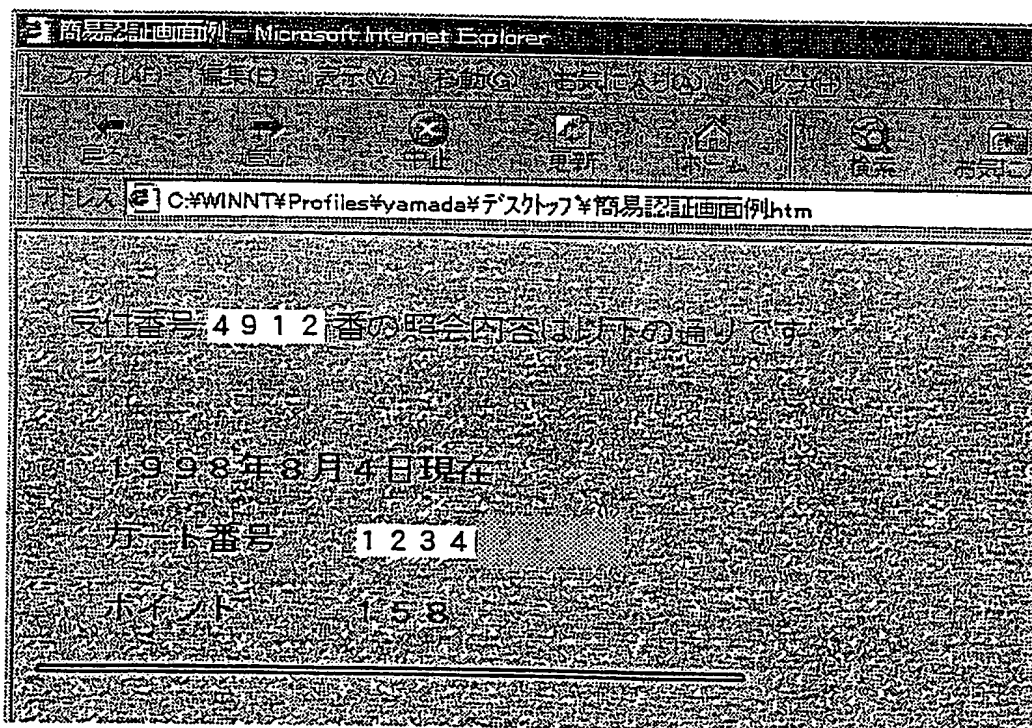
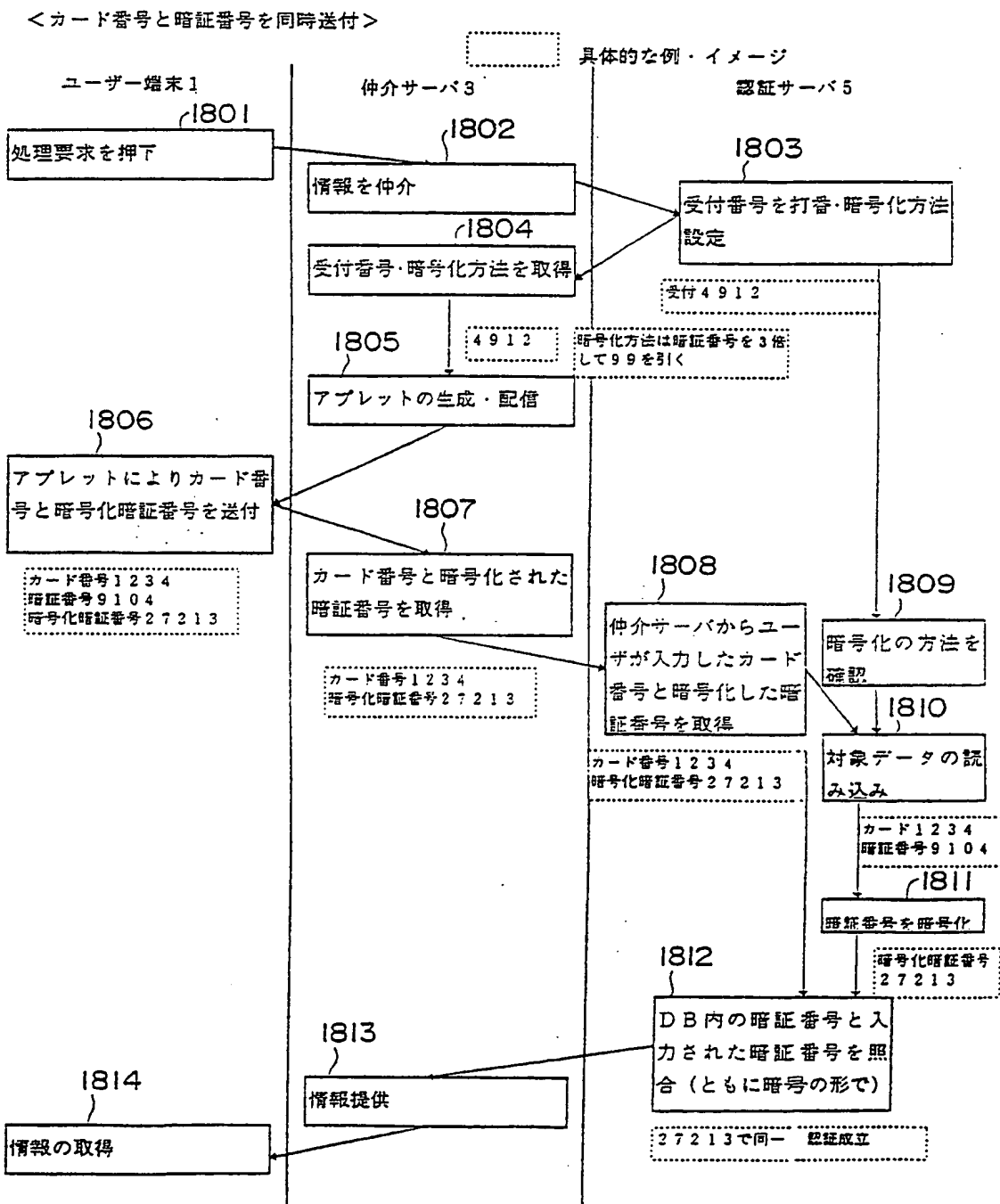


図 17



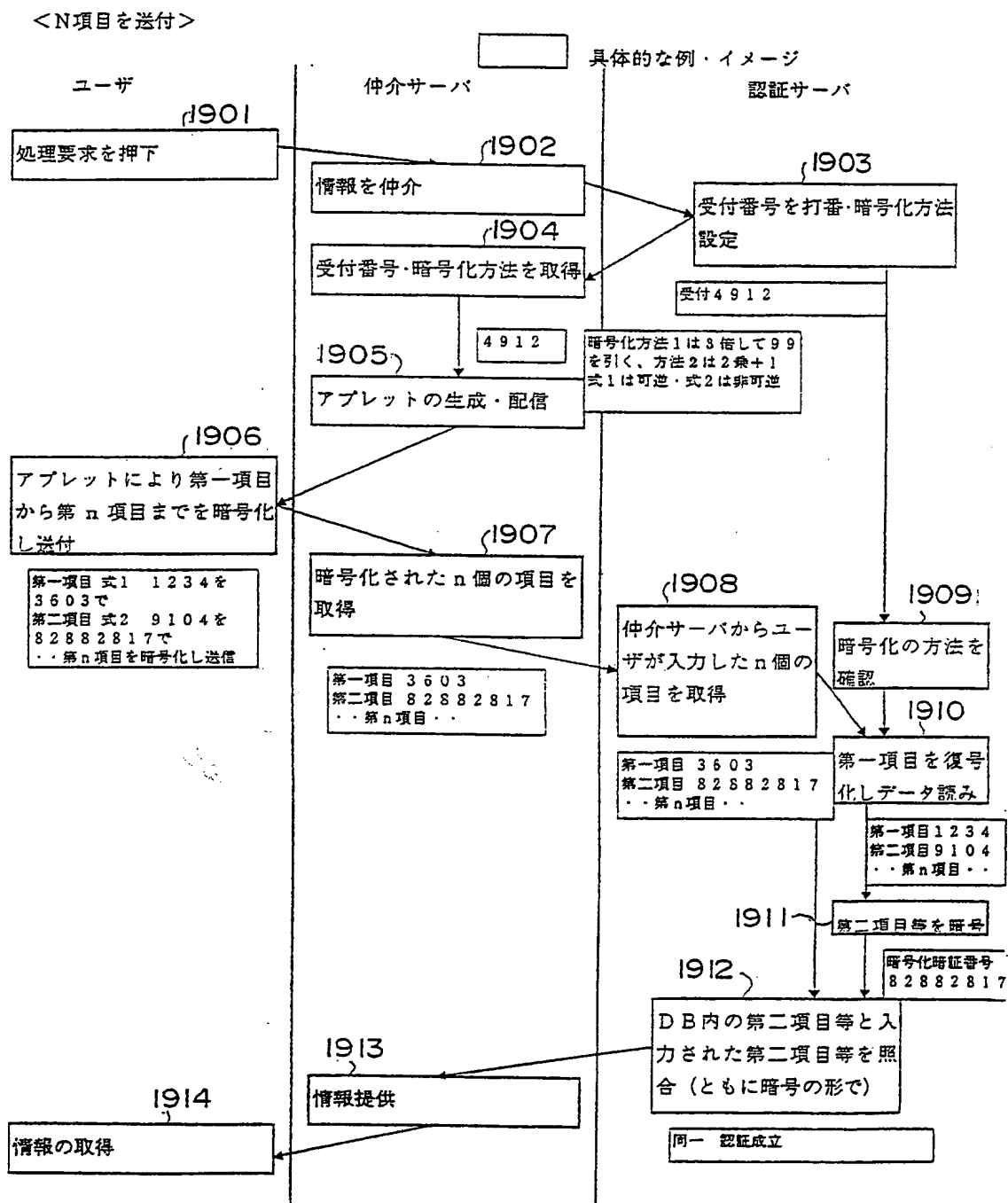
17
11/15/15 Page Blank (uspto)

図 18



This Page Blank (uspto)

図 19



This Page Blank (uspto)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

This Page Blank (uspto)